

Amendments to the Specification

Please replace paragraph [0039] with the following paragraph:

[0039] Embodiments of the invention provide for faster execution of data ciphering in comparison to current approaches. As will be described in more detail below, in various embodiments of the invention, a data ciphering scheme is implemented by overlapping operations to generate different output blocks of data through use of speculative execution of ~~at least certain of the~~ memory accesses. In one such embodiment, data ciphering based on RC4 is employed such that the memory storing the S-box (which stores data needed for the RC4 operations) is more fully utilized. RC4 is a data ciphering scheme in which output blocks are weakly coupled, such that there is a relatively low probability that collisions will occur between data used to generate such different output blocks. While embodiments are described in which RC4 is employed, alternative embodiments may employ different data ciphering schemes in which neighboring output blocks are weakly coupled (where the output blocks are generated in an order and the generation of those output blocks that are in close proximity to each other according to that order are weakly coupled). However, embodiments of the invention are not limited to such data ciphering schemes, as embodiments can be incorporated into any of a number of different types of data ciphering schemes (such as Advanced Encryption Standard (AES), RC5, Data Encryption Standard (DES) etc.).